Office of the Legislative Auditor

State of Montana

Report to the Legislature

October 1993

EDP Audit Report

Information Processing Facility and Central Applications

Each year the Office of the Legislative Auditor audits the central computer facility and centralized computerized applications. This report is used by financial-compliance and performance auditors and contains our conclusions and/or recommendations for improving general controls over the mainframe computer center (Information Processing Facility) and application controls over the following systems:

- State Payroll System
- Statewide Budgeting and Accounting System
- Warrant Writing System

Direct comments/inquiries to:
Office of the Legislative Auditor
Room 135, State Capitol
PO Box 201705
Helena Montana 59620-1705

93DP-33

EDP AUDITS

Electronic Data Processing (EDP) audits conducted by the Office of the Legislative Auditor are designed to assess controls in an EDP environment. EDP controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. In performing the audit work, the audit staff uses audit standards set forth by the United States General Accounting Office.

Members of the EDP audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business and public administration and computer science.

EDP audits are performed as stand-alone audits of EDP controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of four members of the Senate and four members of the House of Representatives.

MEMBERS OF THE LEGISLATIVE AUDIT COMMITTEE

Senator Greg Jergeson, Chairman
Senator Gerry Devlin
Senator Eve Franklin
Senator Tom Keating

Representative John Cobb, Vice Chairman
Representative Ernest Bergsagel
Representative Linda Nelson
Representative Robert Pavlovich

Office of the Legislative Auditor

EDP Audit

Information Processing Facility and Central Applications

Members of the audit staff involved in this audit were: Pete Brustkern, Shawn F. Bubb, Ken Erdahl, Cindy S. Jorgenson, Maureen G. Leo, Rich McRae, Doug G. Melton, Emlyn Neuman-Javornik, and Jill Olson.

STATE OF MONTANA

Office of the Legislative Auditor

STATE CAPITOL
HELENA, MONTANA 59620
406/444-3122

LEGISLATIVE AUDITOR:
SCOTT A. SEACAT

LEGAL COUNSEL:
JOHN W. NORTHEY

DEPUTY LEGISLATIVE AUDITORS:

MARY BRYSON
Operations and EDP Audit

JAMES GILLETT
Financial-Compliance Audit

JIM PELLEGRINI
Performance Audit

October 1993

The Legislative Audit Committee
of the Montana State Legislature:

This is our EDP audit of controls relating to the state's centralized data processing systems operated by the Department of Administration and the State Auditor's Office. We reviewed the Department of Administration's general controls over the Information Processing Facility. Effective July 1, 1993, the legislature transferred the State Payroll application to the department's Personnel Division. We reviewed the department's application controls over State Payroll and the Statewide Budgeting and Accounting System (SBAS). In addition, we reviewed application controls over the Warrant Writer system, operated by the State Auditor's Office. This report contains recommendations for improving EDP controls related to SBAS, State Payroll, and Warrant Writer systems. Written responses to our audit recommendations are included in the back of the report.

We thank the Department of Administration and State Auditor's Office for their cooperation and assistance throughout the audit.

Respectfully submitted,

Scott A. Seacat
Legislative Auditor

Table of Contents

Appointed and Administrative Officials

Department of Administration

Lois Menzies, Director

Dave Ashley, Deputy Director

Connie Griffith, Administrator
Accounting and Management Support Division

Mike Trevor, Administrator
Information Services Division

Mark Cress, Administrator
Personnel Division

John McEwen, Chief
Classification and Pay Bureau

Donna F. Warner, Payroll Manager
State Payroll

Office of the State Auditor

Mark O'Keefe, State Auditor

Dave Hunter, Deputy State Auditor

Thomas L. Crosser, Deputy
Fiscal Control and Management Department

Report Summary

Introduction

Our EDP Audit reviewed centralized controls over the state's mainframe computer and three computer based applications: State Payroll, Warrant Writer, and the Statewide Budgeting and Accounting System (SBAS). We performed a general control review of the state's mainframe computer and application reviews of State Payroll and SBAS, each operated by the Department of Administration. We also performed an application review of Warrant Writer which is operated by the State Auditor's Office. A discussion of general and application controls is included on pages 1 and 2. The objectives and scope of the audit are discussed on pages 2 and 3 of the report.

General Controls

The Department of Administration, Information Services Division (ISD), manages central data processing services for state government. Processing is performed on an IBM 3090 computer operating 24 hours a day except for times allocated for system maintenance.

In our review of ISD's general control environment, we found organizational, procedural, hardware, software, and access controls existed and were operating as intended. We continue to have concerns regarding the department's ability to restore data processing operations following a disaster. The department's disaster recovery plan is not finalized, but we recognize the department's efforts to pursue improvements in its disaster recovery plan. We make no recommendations at this time.

Application Controls

We performed application reviews of the State Payroll, Warrant Writer, and SBAS applications. We reviewed input, processing, and output controls for each application. Overall, we concluded the controls over the applications are adequate to ensure data integrity. However, we found areas where State Payroll and Warrant Writer application controls could be enhanced to further ensure the security and integrity of the application's data. These areas include wage garnishment procedures and electronic access controls. Additional discussion of these and other issues is included in Chapters II and III of the report.

Wage Garnishment Procedures

Levying officers submit written orders to the Department of Administration which require State Payroll to withhold funds from employee salaries. Each pay period, department personnel withhold employee paychecks for outstanding taxes, child support, student loans, or other debts. Once payroll processes, State Payroll submits the withheld funds, or garnisheed wages, to levying officers and provides the employee a paycheck for the remaining portion.

We reviewed garnishment procedures and identified issues where the department did not calculate garnishments in accordance with state and federal regulations. We also determined the department could improve overall efficiency of biweekly garnishment processing procedures.

User Access Should Agree to Job Needs

The State Auditor's Office assigns employee access to various on-line screens depending upon the employee position description. The access allows employees to view or change on-line screen information. We found seven employees have access inconsistent with their job duties. These employees could change warrant payee information and issue warrants to unauthorized individuals. One employee could also change the number and amount of checks written through the Warrant Writer system. The employee reconciles Warrant Writer activity to SBAS each month and could adjust information to ensure the two systems agree.

Industry standards recommend management limit employee access to data required to perform job duties. Because of access concerns we identified, employees are in a position to perpetrate and conceal errors and irregularities.

Chapter I - Introduction

Introduction

We perform an annual electronic data processing (EDP) audit of the state's centralized data processing systems. We review centralized controls over the state's mainframe computer and three computer based applications: State Payroll, Warrant Writer, and the Statewide Budgeting and Accounting System (SBAS). During fiscal year 1992-93, the State Auditor's Office was responsible for operation, maintenance, and control of the State Payroll application. Effective July 1, 1993, the legislature transferred State Payroll to the Department of Administration, Personnel Division.

We performed audit work at the Department of Administration which maintains the state's mainframe, State Payroll, and SBAS. We also performed audit work at the State Auditor's Office which has primary responsibility for Warrant Writer. During our annual audit we gathered information, evaluated controls, and identified risks related to these systems. The controls we identified and tested are relied upon during financial-compliance, performance, and EDP audits for fiscal year 1992-93.

EDP Audit General and Application Controls

An EDP audit consists primarily of a review of internal controls. In an automated environment the procedures for reviewing controls are different from those used in a manual environment. However, the objective of ensuring the reliability of controls is still the same. EDP auditing may entail performing a general and an application control review. The general control review consists of an examination of the following controls and objectives:

Organizational - No one person should be able to conceal material errors or irregularities.

Procedural - Daily operations should protect against processing errors.

Hardware and Software - Hardware and systems software should identify system malfunctions and maintain operations.

System Development - System design and maintenance activities should promote system control and integrity.

Physical Controls - Loss or destruction of assets and records should be prevented and continuous operations should be assured.

Access - Access to hardware and electronic information should be limited to authorized individuals.

A general control review provides information regarding the ability to control EDP applications. Application controls are specific to a given application or set of programs that accomplish a specific objective.

Application controls consist of an examination of the following controls and objectives:

Input - Ensure all data is properly encoded to machine form, all entered data is approved, and all approved data is entered.

Processing - Ensure all data input is processed as intended.

Output - All processed data is reported and properly distributed to authorized individuals.

A review of the application documentation and audit trail is also performed. Applications must operate within the general control environment in order for reliance to be placed on them.

Audit Objectives

The objectives of this EDP audit were to determine the adequacy of:

1. General controls specific to the state mainframe computer.

2. Application controls in order to evaluate the adequacy and accuracy of data processed by SBAS, State Payroll, and Warrant Writer applications.

Audit Scope and Methodology

The audit was conducted in accordance with government audit standards. We compared existing general and application controls against criteria established by the American Institute of Certified Public Accountants (AICPA), General Accounting Office (GAO), and the EDP industry.

We reviewed Department of Administration's general controls related to the state mainframe environment. We interviewed department personnel to gain an understanding of the hardware and software environment at the Department of Administration. We also examined documentation to supplement and confirm information obtained through interviews.

We examined procedures within the mainframe environment which ensure computer processing activities are controlled. For example, we determined mainframe equipment is maintained in a secured area and access is limited to authorized personnel. We also reviewed job control procedures to help ensure integrity of all system processing.

We conducted application reviews over State Payroll, Warrant Writer, and SBAS. We interviewed employees of the Department of Administration and the State Auditor's Office to determine policies and procedures. We reviewed input, processing, and output controls for these systems. We also reviewed supporting documentation to determine if controls over data are effective as well as adequate to ensure the accuracy of data during processing phases.

Controls over centralized operations are supplemented by controls established at user agencies. We did not review controls established by agency users.

Compliance

We determined compliance with applicable state laws and rules and Montana Operations Manual policies. Except as discussed on pages 10 to 13, we found the Department of Administration and the State Auditor's Office to be in compliance with applicable laws and state policy.

Prior Audit Recommendations

Our prior audit report for fiscal year 1991-92 included six recommendations still applicable to the Department of Administration. The department concurred with all six recommendations. We reviewed the status of these recommendations during our audit and determined the department implemented four recommendations and partially implemented two. The recommendations partially implemented concern disaster recovery procedures for SBAS and limiting programmer access to SBAS production programs and data files. These issues are discussed below.

Our prior audit report also included six recommendations applicable to the State Payroll application operated by the State Auditor's Office. The office concurred with our recommendations. During our audit, we determined the office implemented three recommendations and partially implemented three. The partially implemented recommendations concern State Payroll disaster recovery procedures, procedures manuals, and limiting programmer access to production programs and data files. As discussed on page 1, these issues now apply to the Department of Administration and are discussed below.

Programmer Access should be Restricted

During our previous audit we noted Department of Administration programmers had write access to SBAS and State Payroll application programs and data files. We recommended the Department of Administration and State Auditor's Office develop alternative procedures to limit programmer access to production programs and data files.

Industry standards state programmers do not need access to system or application libraries which would provide a means of bypassing controls. Their activities should be restricted to test programs and files, with access only to those programs and files needed for a given assignment. Access to production programs and data files could allow programmers to add fictitious payments and change control total balancing programs to disguise differences. The potential exists for unauthorized and untraceable manipulations of critical information.

We determined the Department of Administration's Information Services Division has initiated a review of security related procedures for all application systems they support. The department is continuing to develop alternative procedures to restrict programmer access to application programs and data files.

Procedures Manual should be Completed

During our previous audit, we reviewed State Payroll procedure manuals and determined the manuals did not provide complete explanations of duties necessary to process biweekly payroll. We recommended the State Auditor's Office complete procedure manuals which clearly define daily duties and problem resolution procedures.

In our current review we determined the State Payroll manager is working to complete a procedure manual which will support the duties of payroll manager and assistant manager. A complete procedure manual should provide a source of reference and enable backup or new employees to perform payroll duties properly and process payroll within established time periods.

Disaster Recovery Procedures should be Completed

During our previous audit, we determined disaster recovery plans for SBAS and State Payroll applications should be updated and tested. We recommended the Department of Administration include On-line Edit & Entry (OE&E) in its SBAS disaster recovery plan. We also recommended the payroll disaster recovery plan include on-line payroll and on-line forms applications. Agencies use OE&E, on-line payroll, and on-line forms applications to electronically input and transfer data to SBAS and State Payroll, respectively.

During our current audit we determined the department has identified basic recovery requirements for OE&E and alternative procedures to follow until mainframe recovery is completed. The department has not established procedures for State Payroll on-line applications but is working with Information Services Division to establish a disaster recovery plan.

The Montana Operations Manual (MOMS) section 1-0240.00 outlines agency responsibilities regarding disaster recovery. These procedures include assigning recovery team member responsibilities; assessing the information and resource requirements necessary to maintain the application; and determining alternate procedures which may be necessary if the recovery cannot be completed timely. In addition, all policies and procedures should be thoroughly and adequately documented.

Documented and tested recovery procedures help normal operations to resume as quickly as possible following a disaster. Without a documented and operable disaster recovery plan, the department may be unable to efficiently process SBAS or State Payroll data.

We recognize thorough disaster recovery planning is an intensive and ongoing process. However, adequate recovery procedures will ensure continued data processing operations and the department's compliance with section 1-0240.00, MOM.

Chapter II - Department of Administration

Introduction

The Department of Administration operates the Information Processing Facility, the Statewide Budgeting & Accounting System (SBAS), and the State Payroll application. This chapter summarizes our review of general controls over the Information Processing Facility and application controls over SBAS and State Payroll.

Information Processing Facility

The Department of Administration, Information Services Division (ISD), manages central data processing services for state government. Central data processing services include, but are not limited to: central mainframe computer processing; design, development, and maintenance support of data processing applications; and disaster recovery facilities for critical data processing applications. Processing is performed on an IBM 3090 computer operating 24 hours a day except during scheduled system maintenance.

General controls, as defined on page 1, are developed by management to ensure computer operations function as intended. In our review of ISD's general control environment, we found overall general controls existed and were operating as intended. However, as discussed in the following section, the department could improve physical security controls by completing disaster recovery procedures.

Mainframe Disaster Recovery Procedures

Disaster recovery procedures provide for continuation of operations following a disaster. User agencies are responsible for recovery of their computer applications following a disaster. ISD is responsible for recovery of the central computer center.

A timely recovery from a major disaster essentially requires a backup facility similar to ISD's computer center. In February 1992, ISD established a five year contract for a backup hotsite with Weyerhauser Corporation in Seattle, Washington. With an annual cost of $28,435, the hotsite agreement provides ISD an alternative location and equipment necessary to recover computer operations. Although ISD performed testing at the hotsite in September 1993, it does not have a finalized disaster recovery plan. In the event of a major disaster, ISD may be unable to recover the state mainframe computer processing functions. The current plan provides for backup recovery using a computer operated by the Department of Justice and located at the National Guard Armory. The backup computer does not have sufficient capacity to operate all critical mainframe applications.

ISD is continuing its efforts to develop disaster recovery plans and procedures. When tested and fully operational, we believe the new hotsite agreement will significantly improve ISD's ability to recover the mainframe computer. Since the department realizes the importance of and continues to pursue improvements in its disaster recovery plan, we make no recommendation at this time.

Statewide Budgeting and Accounting System

The Department of Administration, Accounting Bureau, operates the Statewide Budgeting and Accounting System (SBAS). SBAS is an accounting system which provides financial information used to review and control agency financial transactions. The system also provides agency management budgetary control data used for decision making. SBAS provides uniform accounting and reporting for all state agencies by showing receipt, use, and disposition of all public money and property in accordance with generally accepted accounting principles (GAAP).

The Property Accountability and Management System (PAMS) is a subsystem of SBAS. PAMS is used to account for fixed assets owned by state agencies. A detailed description of the PAMS system, and statewide policies for property accounting are contained in Chapter 1700 of the Montana Operations Manual.

We performed an application review of SBAS. We reviewed input, processing, and output controls over SBAS. Overall, we determined controls over SBAS were effective, as well as adequate, to ensure data integrity during processing phases for fiscal year 1992-93.

State Payroll System

The State Payroll System processes payroll for all state agencies except six university system units. Each of the six university units processes its own payroll. Payroll warrants for Montana State University and the University of Montana are printed and distributed at those locations. The four remaining university system units process warrants through SBAS and Warrant Writer but not through State Payroll.

Our review was limited to payroll transactions processed through the State Payroll System. We did not examine controls over payroll processing or distribution at the six university system units.

The State Payroll System is also referred to as the Payroll/Personnel/Position Control system (P/P/P). The payroll component issues and tracks state of Montana employees' wage and benefit payments. The payroll component also calculates payroll deductions, leave and service adjustments, automatic salary increases, and direct bank deposits upon request.

The personnel component records detailed information about each state employee. The personnel database includes information on birth, sex, disability, and emergency notification for each employee. The personnel database also includes information to verify compliance with state and federal labor laws.

The position control component provides management with information necessary for budgeting purposes. The position control component database includes information on employee position number, grade, classification code, date of hire, and longevity. The database also includes information on the amount of money budgeted for specific positions and the portion of budgeted amounts that have been expended for those positions.

We performed an application review over the State Payroll System. We did not test controls over the position control or personnel components. Controls for these systems are discussed in our performance audit report of the P/P/P System (89P-36) issued February 1990.

We reviewed input, processing, and output controls over the State Payroll System. Overall, we determined input, processing, and output controls were effective for fiscal year 1992-93. However, we found areas where controls could be enhanced to further ensure data security and integrity. The following sections summarize our findings.

Wage Garnishment Procedures

Levying officers submit written orders to the Department of Administration which require State Payroll to withhold funds from employee salaries. Each pay period, department personnel withhold employee paychecks for outstanding taxes, child support, student loans, or other debts. Once payroll processes, State Payroll submits the withheld funds, or garnisheed wages, to levying officers and provides the employee a paycheck for the remaining portion.

We reviewed garnishment procedures and identified issues where the department did not calculate garnishments in accordance with state and federal regulations. We also determined the department could improve overall efficiency of biweekly garnishment processing procedures. These issues are discussed in the following sections.

Wage Garnishments should be Computed According to State and Federal Regulations

Section 25-13-614, MCA, and federal regulations outline wage garnishment calculations and define disposable earnings as the portion of wages subject to garnishment. Disposable earnings represent gross pay less mandatory deductions (such as state and federal taxes). Savings deductions and other voluntary withholdings are included as disposable income. In addition, child support payments, even if court ordered, must be included in disposable earnings.

In five of nine cases we reviewed, we determined the department did not calculate disposable income in accordance with state and federal regulations. We noted department personnel calculated disposable income by subtracting deferred compensation and/or child support from gross pay. As a result, the office understated disposable income and under-withheld garnishments between $1.24 and $60.90 per case during the pay period we reviewed.

We discussed this issue with department personnel. The department agrees that deferred compensation should not be deducted from disposable income. An official indicated the department accidentally excluded deferred compensation from the calculations. However, the official indicated excluding child support from disposable income is consistent with state policy to ensure top priority for the Child Support program. We believe the department could deduct child support after calculating disposable income in accordance with state and federal regulations.

In one of the remaining four cases, the department properly calculated disposable earnings but garnisheed wages $120.20 less than allowed by law. The employee had established regular voluntary savings deductions totalling $450 per paycheck. State Payroll personnel indicated the department cannot withhold voluntary deductions without the employee's authorization. As a result, employees may establish voluntary deductions to avoid legal obligations and therefore protect wages from garnishment. Based on our review of state law and federal regulations, we determined the department does not need an employee's authorization to withhold the employee's wages.

Recommendation #1

We recommend the Department of Administration calculate disposable income and garnisheed wages in accordance with state and federal regulations.

Processing Fees Exceed Garnisheed Wages

State Payroll requires levying officers to formally notify employees each pay period when their paycheck will be garnisheed. Levying officers charge employees $17 to $24 for each garnishment notification. Levying officers subtract this fee from an employee's withheld wages prior to satisfying the garnishment order.

In one of nine garnishment cases we reviewed, we found the employee's available disposable income, as calculated by State Payroll, did not cover the processing fee. As a result, the employee's outstanding debt continues to increase with each formal notification.

We determined state and/or federal laws and regulations require only one written order for each garnishment request. Currently, the employee pays $17 to $24 each pay period per garnishment notification. Department personnel indicated they require levying officers to submit a written order each pay period to avoid garnisheeing wages after a debt is satisfied. However, the levying officer will formally notify State Payroll to stop garnisheeing wages. The department indicated it will examine this issue.

Recommendation #2

We recommend the Department of Administration execute garnishment requests upon one written order.

Automating Wage Garnishment Procedures would Improve Efficiency

After the department completes payroll processing, a State Payroll employee retains payroll checks which are subject to garnishment. The employee manually calculates disposable earnings to determine the portion available for garnishment. Department personnel process a replacement payroll warrant for the remaining portion and deposit the original warrant in the State Treasury.

Section 25-13-614, MCA, specifies the maximum portion of an employee's disposable income subject to garnishment. The law identifies several restrictions and/or tests the department employee must apply against disposable income in order to determine the allowable wage garnishment. Department personnel indicated it takes one employee forty hours each pay period to manually complete wage garnishment procedures.

Each pay period, the department processes 45 to 50 employee garnishments. Of this amount, approximately 42 garnishments repeat every pay period. We believe the department's current procedure for processing replacement payroll warrants is inefficient and increases the risk original warrants will be lost or stolen. The department could develop a microcomputer program to calculate wage garnishments or modify the State Payroll application to automatically deduct garnisheed wages from the employee's original paycheck.

We believe automated processing, at minimal cost to the department, could improve employee efficiency and ensure consistent and accurate calculations in accordance with state and federal law. The department indicated it will consider alternative procedures to automate the wage garnishment procedures.

Recommendation #3

We recommend the Department of Administration examine alternatives and automate the biweekly wage garnishment procedures.

Chapter III - State Auditor's Office

Introduction

The State Auditor's Office operates the Warrant Writer System. This chapter summarizes our audit of application controls over the Warrant Writer System and identifies areas where controls could be improved.

Warrant Writer System

The Warrant Writer system controls creation and distribution of most state warrants and the redemption of all state warrants. The system accounts for state warrants issued, outstanding, and redeemed.

The State Auditor's Office and the Department of Administration jointly operate and maintain Warrant Writer. However, the State Auditor's Office is primarily responsible for the system. Department of Administration initiates warrant writing and reconciles issued warrants to SBAS. The State Auditor's Office prepares warrants, distributes warrants, and reconciles warrants outstanding to SBAS. Both departments jointly control warrant redemption.

We performed an application review over the Warrant Writer system. We reviewed input, processing, and output controls over Warrant Writer. Overall, we determined controls over Warrant Writer are effective, as well as adequate, to ensure accuracy of data during processing phases. However, we found areas where controls could be enhanced to further ensure data security and integrity. This chapter summarizes our review of the Warrant Writer system.

Electronic Access Controls

Access controls provide electronic safeguards designed to protect computer system resources. The State Auditor's Office uses access control software called Access Control Facility-2 (ACF2) to control electronic access to Warrant Writer data stored on the mainframe computer. In addition, the office controls access through security programs within Warrant Writer which control access to specific screens (menus used to add, change, or delete warrant data). We reviewed access security and identified areas where the office should improve access controls over Warrant Writer screens.

User Access should Agree to Job Needs

The State Auditor's Office assigns employee access to various on-line screens depending upon the employee position description. The access allows employees to view or change on-line screen information. For example, prior to processing warrants, employees view and offset (withhold) warrants written to individuals or corporations who owe money to the state of Montana. We found nine office employees with access to Warrant Writer.

We reviewed access privileges for the nine users and found seven with access inconsistent with their job duties. Seven employees can change warrant payee information, including payee identification number, name, address, and direct deposit bank account number. These employees could change payee information and issue warrants to unauthorized individuals.

Two of the seven employees tested have access which allows them to offset warrants. These employees could offset warrants and change the recipient name and address. We determined the employees only need to view offset information to answer questions concerning warrant status.

One of the seven employees has inappropriate access to Warrant Writer information. The access allows the employee to change the number and amount of checks written through the Warrant Writer system. The employee reconciles Warrant Writer activity to SBAS each month and could adjust information to ensure the two systems agree. The employee noted access to this screen is not needed to perform the employee's job duties.

Industry standards recommend management limit user access to data files required to process or maintain an application in the performance of their job duties. Because of access concerns we identified, employees are in a position to perpetrate and conceal errors and irregularities.

To improve access controls, we believe the office should complete a formal review of access over Warrant Writer. Although the office reviewed employee access privileges in

March 1992, the office could not provide complete documentation of the review. We believe a complete and documented review would identify existing access problems. Established review procedures could ensure employee access agrees to position duties and management's authorization.

Recommendation #4

We recommend the State Auditor's Office:

A. Eliminate inappropriate access to the Warrant Writer System.

B. Perform and document a formal access review over the Warrant Writer System to ensure access agrees with employee job responsibilities.

Warrant Distribution Procedures should be Improved

The State Auditor's Office maintains signature cards which office personnel review to verify agency employees are authorized to pick up payroll or other warrants. We identified concerns regarding State Auditor's Office warrant distribution procedures. We observed instances where office personnel distributed warrants to unauthorized individuals and/or did not obtain authorized signatures.

We determined an unauthorized agency employee attempted to pick up payroll warrants. According to State Auditor's Office authorization cards, the employee was not authorized to receive payroll warrants. Office personnel did not question the employee's authorization until we brought it to their attention. Office personnel indicated they were not aware the agency employee was no longer authorized to receive payroll warrants.

We also noted the State Auditor's Office released a warrant to an agency employee even though office personnel were aware the employee was not authorized to pick up the warrant. A State

Auditor's Office employee stated there are cases when the office will release warrants to unauthorized individuals.

In another instance, an individual signed for only two of three warrants issued by a State Auditor's Office employee. We determined an office official detected the error while reviewing the signature log and brought the error to the employee's attention. However, when we questioned office personnel, they indicated the individual picking up warrants is responsible to sign for all warrants received.

Industry guidelines suggest management follow procedures to ensure computer application output (warrants) is distributed to authorized individuals. Although office policy requires only authorized individuals receive warrants, the instances we noted indicate employees do not consistently follow office policy. As a result, warrants could be obtained by unauthorized individuals which increases the risk of theft or misuse. We discussed these issues with the State Auditor's Office. Office management stated the office has changed its warrant distribution procedures and will clarify its policy concerning exceptions to distribution procedures.

Recommendation #5

We recommend the State Auditor's Office review warrant distribution procedures and clarify office policy to ensure warrants are properly distributed.

Access to Vault Storage Area should be Restricted

The State Auditor's Office uses a mechanical combination lock and key to restrict access to a vault area located near its mailroom. The office stores blank warrant stock and a signature plate inside the vault. To access the vault, an employee must enter the correct combination code and key at the vault entrance. An additional key is required to access the signature plate. The office stores keys for the vault and signature plate in a locked box outside the vault area.

During our review, we found the office has provided a vault key and combination code to four employees. Three of the employees also have a key to the locked box which contains the signature plate key. As a result, the employees could individually access blank warrant stock and the signature plate and create fictitious warrants. Montana Operations Manual (MOMS) section 2-1210.00 states no one person should be in a position to perpetrate and conceal errors and irregularities.

We discussed our concerns with office personnel. The office indicated it would change procedures to ensure no one person has unlimited access to the warrant vault area.

Recommendation #6

We recommend the State Auditor's Office evaluate key assignment and improve access controls to the vault storage area and signature plate.

Access to Invalid Warrants should be Controlled

State Auditor's Office personnel mark "spoiled" on warrants which are damaged either during processing, by the postal service, or by the recipient. The office temporarily stores these warrants in the mailroom area until office personnel file the warrants. We reviewed warrants stored in the mailroom and found one of five damaged warrants was not voided.

Although office policy outlines procedures for voiding warrants, an office employee could not explain why the warrant was not voided. Unless these warrants are voided upon receipt, an individual could inappropriately cash the warrants.

During previous audits the mailroom was a restricted area; however, during this audit we noted mailroom access is no longer limited to specific employees. Office personnel indicated they no longer restrict mailroom access to allow employees to perform their duties more efficiently. Because changes in the office's mailroom access policy reduce controls, we believe the office should implement stronger controls over damaged, incorrectly processed, or returned warrants.

Recommendation #7

We recommend the State Auditor's Office follow established controls to prevent unauthorized access to spoiled warrants stored in the mailroom.

Disaster Recovery Plan should be Complete

The State Auditor's Office does not have a complete written disaster recovery plan for the Warrant Writer application. Although the office has an agreement with Department of Administration's Application Services Bureau for software support and recovery, the agreement does not include recovery of warrant writer data or address State Auditor's Office responsibilities.

Management should maintain adequate written recovery procedures for critical applications to ensure a rapid system recovery from either short-term interruption or major catastrophe. The Montana Operations Manual (MOMS) section 1-0240.00 outlines agency responsibilities regarding disaster recovery which include assigning recovery team member responsibilities; assessing the information and resource requirements necessary to maintain the application; and determining alternate procedures which may be necessary if the recovery cannot be completed timely. Documented and tested recovery procedures allow normal operations to resume as quickly as possible following a disaster. Without a complete disaster recovery plan, the office may be unable to electronically process warrants.

A State Auditor's Office official indicated the office has not had time to review disaster recovery procedures since the recent change in administration. However, the official has agreed to complete disaster recovery procedures. We believe the benefits provided by an effective disaster recovery plan exceed the costs of developing the plan. The office should define team member assignments, application requirements, alternative procedures, etc., for the Warrant Writer application.

Recommendation #8

We recommend the State Auditor's Office complete its Warrant Writer application disaster recovery plan in accordance with state policy.

Agency Responses

DEPARTMENT OF ADMINISTRATION
DIRECTOR'S OFFICE

MARC RACICOT, GOVERNOR

MITCHELL BUILDING

STATE OF MONTANA

(406) 444-2032
FAX 444-2812

PO BOX 200101
HELENA, MONTANA 59620-0101

November 17, 1993

Scott A. Seacat
Legislative Auditor
Office of the Legislative Auditor
State Capitol
Helena, MT 59620

Dear Mr. Seacat:

Following are responses to the recommendations in Chapter II of the Audit Report on Information Processing Facility and Central Applications.

Recommendation #1

We recommend the Department of Administration calculate disposable income and garnished wages in accordance with state and federal regulations.

We concur. Beginning with the November 24, 1993 payday, we will not exclude child support payments from disposal income.

Recommendation #2

We recommend the Department of Administration execute garnishment requests upon one written order.

We do not concur. We agree that only one written notice is legally necessary. However, our examination of the levying process indicates that the Department would incur additional expense and liability in implementing this recommendation. The department would need to develop further recordkeeping procedures to track the biweekly pay down of the levy and for those employees with multiple levies. Procedures for notice to the Department when the employee satisfies the debt in some other way would also be needed. We would also need to decide whether to keep the biweekly withholding until the levy is satisfied or forward it biweekly to the levying officer. An effect of implementing this recommendation is that the Department would take on work currently performed by the levying officer.

"AN EQUAL OPPORTUNITY EMPLOYER"

Levying officers prefer to serve a written notice for each pay period in order to insure accurate record keeping, to deal with other actions affecting the debt and to meet their obligations to report to the debt holder and the court. The fee charged by a levying officer is not regulated. The act of requiring only one order that must be carried out over several pay periods would likely lead to higher fees for the record keeping and reporting that the levying officer performs.

Collection of debt is a quagmire. It is time consuming, subject to error, involves intricate legal procedures and is emotional. With the current procedure, the levying officer bears the majority of the responsibility for the process. We prefer to keep it that way.

Recommendation #3

We recommend the Department of Administration examine alternatives and automate the biweekly wage garnishment procedures.

We concur. The Department implemented an automated procedure using mainframe and PC software with the July 21, 1993 pay day. This procedure has improved accuracy and reduced the time for processing garnishments.

If you have any questions concerning the Department's response, please feel free to contact me.

Sincerely,

Lois Menzies

Lois Menzies
Director

STATE AUDITOR
STATE OF MONTANA

Mark O'Keefe
STATE AUDITOR

COMMISSIONER OF INSURANCE
COMMISSIONER OF SECURITIES

November 12, 1993

Mr. Scott Seacat
Legislative Auditor
Office of the Legislative Auditor
State Capitol Building
Helena, MT 59620

Dear Mr. Seacat:

We have reviewed your EDP audit concerning our Warrant Writer Program application. Our response to each of the audit recommendations follows:

Recommendation #4

We recommend the State Auditor's Office:

A. Eliminate inappropriate access to the Warrant Writer System.

B. Perform and document a formal access review over the Warrant Writer System to ensure access agrees with employee job responsibilities.

Agency Response:

A. We concur. We will immediately change access that we determine inappropriate.

B. We concur. In conjunction with recommendation A, we will initiate a formal review to determine what access is necessary for the performance of each employees' duties.

Recommendation #5

We recommend the state Auditor's Office review warrant distribution procedures and clarify office policy to ensure warrants are properly distributed.

Agency Response:

We concur. We have restructured our warrant distribution process. All warrant distribution is now handled by Warrant Writer personnel. We have revised our exception policy to clarify how an agency can request distribution of warrants to persons not on the current signature cards for that agency.

Recommendation #6

We recommend the State Auditor's Office evaluate key assignment and improve access controls to the vault storage area and signature plate.

Agency Response:

We concur. We have reassigned keys and combinations so that no single person has access to the entire warrant writing area.

Recommendation #7

We recommend the State Auditor's Office follow established controls to prevent unauthorized access to spoiled warrants stored in the mailroom.

Agency Response:

We concur. We have instructed staff to insure security of returned, damaged or voided warrants. We will periodically check to insure continued compliance with these security procedures.

Recommendation #8

We recommend the State Auditor's Office complete its Warrant Writer application disaster recovery plan in accordance with state policy.

Agency Response:

We concur. We have begun the review process of existing disaster recovery procedures and assignments. We understand the importance of this issue and will develop a current plan as soon as possible.

Thank you for the opportunity to respond to the recommendations made by your staff. I would also like to thank your staff for their patience and the professional manner they used working with my staff.

Thank you for your time and energy.

Sincerely,

Mark O'Keefe

Mark O'Keefe
State Auditor

MOK/tcp